Amendments to the Specification

Please replace the paragraph that begins on Page 1, line 5 and carries over to Page 2, line 2 with the following marked-up replacement paragraph:

-- The present invention is related to U. S. Patent _____ (serial number 09/466,625, filed 12/17/1999), titled "Providing End-to-End User Authentication for Host Access Using Digital Certificates", and U. S. Patent _____ (~~serial number 09/_____, filed~~ number 09/619,912, filed concurrently herewith), titled "Technique for Handling Subsequent User Identification and Password Requests with Identity Change within a Certificate-Based Host Session", both of which are commonly assigned to the International Business Machines Corporation (IBM) and which are hereby incorporated herein by reference. --

a1

Please replace the paragraph that begins on Page 3, line 16 and carries over to Page 4, line 4 with the following marked-up replacement paragraph:

-- Digital certificates may be used to authenticate entities, as is well known in the art. U. S. ~~Patent _____ (serial~~ Patent 6,128,728 (serial number 09/064,632, filed 12/10/98), which is titled "Certificate Based Security in SNA Data Flows", teaches a technique whereby digital certificates are transported in appropriate Systems Network Architecture ("SNA") data flows between a client and a host for identifying the user to the host application, but this existing technique requires those host programs which authenticate the user to RACF (or other host access control facility) to be modified to use the certificate instead of the traditional user ID (user identifier) and password. This requires an enterprise to upgrade each of its application subsystems in order to achieve the benefits. So for some enterprises, the previous approach may

a2

PAGE 4/39 * RCVD AT 5/10/2004 4:18:46 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/5 * DNIS:8729306 * CSID:4073437587 * DURATION (mm-ss):10-08

a2

be impractical and unacceptable. --

Please replace the paragraph that begins on Page 34, line 20 and carries over to Page 35, line 14 with the following marked-up replacement paragraph:

-- At some time later, the Web application at browser client 701 indicates a new host application sign-on sequence (which, as described for the first aspect, may be to the same application currently in use or to a different application), as shown at 750. The Web application server 702 may need to solicit the application ID (e.g. using a HyperText Transfer Protocol, or "HTTP", message) from the client 701, if this information is not already available to the server. In response to receiving message 750, the Web application server retrieves the previously-cached certificate (received in flow 705), and sends 755 this certificate (or a reference thereto) along with the application ID to RACF 704 in the same manner which has been described for message 460 of Fig. 4. (Note that the TN3270 server is not required to scan the 3270 data stream for the user ID and password in this aspect, as the correct values are automatically provided by the TN client.) The RACF response, including the generated passticket, is received at 760. The Web application server then uses this information to send 765 to the host application at host system 703. The host application verifies the user's credentials using this passticket and user ID, and traffic between the host application and Web application server proceeds as in the prior art, as shown at 770. The client application 701 then proceeds to interact 775 with the now-current host application. --

a3

Please replace the paragraph on Page 36, lines 4 - 19 with the following marked-up replacement paragraph:

PAGE 5/39 * RCVD AT 5/10/2004 4:18:46 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/5 * DNIS:8729306 * CSID:4073437587 * DURATION (mm-ss):10-08

-- In Fig. 8, receipt of message 855 indicates that the client wishes to use different credentials. As previously discussed, this message may be sent to enable a previously-authenticated user to use different credentials, or to enable a different user to authenticate himself to an application within the same secure session. As indicated in message 855, a new certificate (or, alternatively, a reference thereto) is transmitted from client 801, along with an identifier of the application, in this asynchronous notification. In addition, this message 855 includes additional information that is used to prove that the sender is the legitimate owner of the certificate (i.e. is authorized to use the certificate). The manner in which this message is formatted and in which the authorization proof is provided in this second preferred embodiment is discussed in more detail below, with reference to element 955 of Fig. 9. This new certificate is cached or otherwise stored at server 802, and is forwarded (see message 860) to RACF 804 along with the user ID and application identifier from message 855. The processing of message flows 860 through 880 is analogous to those numbered 460 through 480 in Fig. 4, except that message 860 passes the certificate which was received on message flow 855 instead of the certificate received during the SSL session establishment flows (and the passticket returned at 865 then represents the access privileges of this new certificate). --

Please replace the paragraph that begins on Page 37, line 15 and carries over to Page 38, line 10 with the following marked-up replacement paragraph:

-- The new additional parameters are used, according to the second embodiment of the present invention, as proof to authenticate the identity of the certificate sender. The first of the additional parameters, "CERTIFICATE", is used to convey the contents of a digital certificate.

PAGE 6/39 * RCVD AT 5/10/2004 4:18:46 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/5 * DNIS:8729306 * CSID:4073437587 * DURATION (mm-ss):10-08

The "RSEED..." parameter (see 910) is used to enable the server to pass a random value to the client. The random number value is concatenated to the environment variable name, enabling the server to pass variable data to the client even though an explicit capability for transmitting values from the sender of the DO command is not provided in RFC 1572. For example, if the random number is 1490285673237, then the environment variable is passed from the server in the NEW-ENVIRON SEND command as "USERVAR RSEED1490285673237", and returned from the client in the NEW-ENVIRON IS command as "USERVAR RSEED1490285673237 VALUE". (Note: this example is not intended to be representative of the optimal length of the random seed value.) Both the client and server record the value to be used as the random seed value for later use. The client and server will use this random value, along with a sequence number, to prevent replay attacks. The "AUTHINFO" parameter is used to transmit authentication information from the client to the server, as will now be described. --

---

Please replace the paragraph that begins on Page 40, line 15 and carries over to Page 41, line 5 with the following marked-up replacement paragraph:

-- While ~~the preferred embodiment~~ preferred embodiments of the present invention [[has]] have been described, additional variations and modifications in ~~that embodiment~~ those embodiments may occur to those skilled in the art once they learn of the basic inventive concepts. In particular, alternative data streams (such as a 5250 data stream or a VT data stream) may be used which provide the communications between the user's modern PC-based computer system and the legacy host applications and data. Further, security software other than the IBM RACF software may be used for protecting host-based assets, and techniques other than the RFC 1572

PAGE 7/39 * RCVD AT 5/10/2004 4:18:46 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/5 * DNIS:8729306 * CSID:4073437587 * DURATION (mm-ss):10-08

protocol may be used to convey information between the client and server provided that functionality equivalent to that described herein is supported. Therefore, it is intended that the appended claims shall be construed to include ~~both the~~ a preferred embodiment and all such variations and modifications as fall within the spirit and scope of the invention. –

a6

PAGE 8/39 * RCVD AT 5/10/2004 4:18:46 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/5 * DNIS:8729306 * CSID:4073437587 * DURATION (mm-ss):10-08